**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| In re application of: **Adler et al.** | § | Group Art Unit: **2132** |
| Serial No. **09/884,311** | § | Examiner: **Herring, Virgil A.** |
| Filed: **June 19, 2001** | § | Customer No.: **50170** |
| For: **Using an Object Model to Improve Handling of Personally Identifiable Information** | § | |

**Commissioner for Patents**
**P.O. Box 1450**
**Alexandria, VA 22313-1450**

**ATTENTION: Board of Patent Appeals and Interferences**

## APPELLANTS' BRIEF (37 C.F.R. § 41.37)

This Appeal Brief is in furtherance of the Notice of Appeal filed October 23, 2008 (37 C.F.R. § 41.31).

The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying Fee Transmittal.

## I. Real Party in Interest

The real party in interest in this appeal is the following party: International Business Machines Corporation.

## II. Related Cases

With respect to other appeals and interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

## III. Jurisdiction

The Board has jurisdiction under 35 U.S.C. § 134(a). The Examiner mailed a non-final rejection on July 23, 2008, setting a three-month shortened statutory period for response. The time for responding to the non-final rejection expired on October 23, 2008. Rule 134. A notice of appeal was filed on October 23, 2008. The time for filing an appeal brief is two months after the filing of a notice of appeal. Bd.R. 41.37(c). The time for filing an appeal brief expires on December 23, 2008. The appeal brief is being filed on December 19, 2008.

## IV. Table of Contents



## V. Table of Authorities

## VI. Status of Amendments

No amendment was filed after mailing of the non-final rejection dated July 23, 2008.

## VII. Grounds of Rejection to be Reviewed on Appeal

The grounds of rejection to be reviewed on appeal are:

- the rejection of claims 1 and 2 under 35 U.S.C. §102(b) as being allegedly anticipated by Benantar et al. (U.S. Patent no. 5,787,427);
- the rejection of claim 3 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Benantar et al. in view of Tolopka et al. (U.S. Patent no. 6,044,349); and
- the rejection of claim 19 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Benantar et al. in view of Gifford et al. (U.S. Patent No. 5,614,927).

## VIII. Statement of Facts

**1.** In rejecting claims 1-2, the Examiner cites Figure 5 and column 6, lines 54-67 of Benantar as teaching associating administrator and control access levels to an object group with a user.

**2.** In rejecting claims 1-2, the Examiner states that "rules specifying administration of a data object implies the ability of the first user Alice to provide the data subject to a second user" (July 23, 2008 Office Action, page 2).

**3.** Neither Figure 5 nor column 6, lines 54-67 of Benantar specifically state that administration level access includes an ability of a first user to provide a data subject to a second user.

**4.** Neither Figure 5 nor column 6, lines 54-67 of Benantar specifically state any details regarding operations that may be performed by a user having administration level access.

**5.** In rejecting claim 3, the Examiner states that Tolopka teaches the features of claim 3 at column 6, lines 36-52 (July 23, 2008 Office Action, page 5).

**6.** Column 6, lines 36-52 of Tolopka actually teaches that the user may manually type information with a text editor or other application and download it to the storage medium such that user entered labels may be added to the table

shown in Figure 2, which is a depiction of information categories and information units stored on the storage medium.

**7.** In rejecting claim 19, the Examiner states that Gifford teaches depersonalization of objects (see July 23, 2008 Office Action, pages 5-6) at column 8, lines 1-8.

**8.** Column 8, lines 1-8 of Gifford actually teaches that, after partitioning a database, the correlation between public attributes and private attributes is reduced by camouflaging some highly correlative public attribute values and outright removing some tuples containing highly correlative public attribute values which are difficult to camouflage.

## IX. Argument

### A. Rejection under 35 U.S.C. §102 Based on Benantar

The Office Action rejects claims 1 and 2 under 35 U.S.C. § 102(b) as allegedly being anticipated by Benantar (U.S. Patent No. 5,787,427). This rejection is respectfully traversed.

#### 1. Independent Claim 1

Claim 1 of the present application reads as follows:

1. A method, in a data processing system, for handling personally identifiable information, said method comprising:

providing, in a computer, a first set of object classes representing active entities in an information-handling process, wherein a limited number of privacy-related actions represent operations performed on data and wherein each of the active entities is a human being or legal entity;

providing, in said computer, a second set of object classes representing data and rules in said information-handling process, wherein at least one object class has said rules associated with said data, and wherein said data represents said personally identifiable information; and

processing transactions, in the data processing system, involving said personally identifiable information, using said computer and said first and second set of object classes, so as to enforce a privacy policy, associated with the personally identifiable information and defined by said rules, against one or more active entities represented by said first set of object classes, wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity, wherein:

**a first active entity represented by a first object class in said first set of object classes is a first data user that requests said personally identifiable information from a data subject that is a second active entity represented by a second object class in said first set of object classes,**

**said data subject is an active entity that is personally identifiable by said personally identifiable information;**

**a third active entity represented by a third object class in said first set of object classes is a second data user that requests said personally identifiable information from said first data user, and**

**said rules define if and how said personally identifiable information may be provided, by said first data user, to said second data user.**

(emphasis added)

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102

only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). As first presented in the Response filed on November 14, 2007, Appellants respectfully submit that Benantar does not identically show every element of the claimed invention arranged as they are in the claims. Specifically, Benantar does not teach the features of claim 1 emphasized above, or the similar features found in the other rejected independent claims.

As discussed at length in the November 14, 2007 Response, and again in the Response to Final Office Action filed April 1, 2008 which was entered in response to the filing of the Request for Continued Examination (RCE) filed on April 25, 2008, it should be noted that claim 1 of the present application recites three specific active entities: (1) a first data user that requests personally identifiable information from (2) a data subject, and (3) a second data user that requests the personally identifiable information for the data subject (2) from the first data user (1). The rules define if and how the personally identifiable information (about the data subject (2)) may be provided, by the first data user (1), to the second data user (3). Thus, the rules in the present invention define if and how one party may send information to a second party, the information being descriptive of a third party. Benantar does not provide any such features.

Benantar describes an information handling system in which objects are grouped so that they can share common control access policies. Benantar is

concerned with the large storage requirements of Access Control Lists (ACLs) and alleviates the problems of having to have a lot of storage or memory consumed by ACLs by grouping objects that can use the same access policies on a particular object or set of objects. However the control access policies merely specify the types of actions, or methods, that the particular objects can themselves perform on the object in question, e.g., read, write, execute, use, administer, or control (see column 6, lines 54-67).

In particular Benantar has improved upon the traditional access matrix in which authorization policies are specified by identifying subjects in rows of the matrix and rights in the columns of the matrix with the corresponding authorization policies being specified in the intersection of the row and column (see Benantar, column 3, line 22 to column 4, line 47). The improvement offered by Benantar is to group subjects and then use the groups, rather than the individual subjects, in the access matrix (see Tables 4 and 5 of Benantar). However, in all cases, the resulting authorization policy in the access matrix of Benantar is the same as in the traditional access matrix, i.e. the authorization policy specifies what access the subject has to the object in question.

To the contrary, the rules in claim 1 are not limited to what access the first data user has to the data subject or what access the second data user has to the data subject. Rather, the rules specify if and how the data subject may be provided by the first data user to the second data user. The access mechanisms of Benantar do not cover such functionality. Rather, with Benantar, the access matrix merely specifies what operations the first data user may perform on the data subject, and separately specifies what operations the second data user may perform on the data subject. The access matrix in Benantar does not specify if and how the first data user may send the data subject to the second data user in response to the second

data user requesting the data subject from the first data user.

In other words, Benantar provides mechanisms for controlling access by the data users to the data subject in the manner depicted in Figure A of the Evidence Appendix. As can be seen from Figure A, the ACLs or access matrix of Benantar only addresses each individual data user, or "subject" in Benantar, access to the data subject. To the contrary, the rules recited in claim 1 of the present application provide a mechanism for controlling access by the data users to the data subject in the manner depicted in Figure B of the Evidence Appendix.

As can be seen from Figure B, the rules of the invention recited in claim 1 control the transfer of the data subject from the first data user to the second data user. Benantar is not even concerned with such transfers of information, let alone provides any mechanism for controlling such transfers of information. The ACLs in Benantar only govern the direct access that the specified user has to the group of objects (equated to Appellants' data subject by the Examiner) and does not provide any control such as that recited in claim 1, i.e. control over the transfer of the data subject from the first data user to the second data user.

Thus, in view of the above, Appellants respectfully submit that Benantar does not teach each and every feature of independent claim 1 as is required under 35 U.S.C. § 102(b). At least by virtue of its dependency on claim 1, Benantar does not teach each and every feature of dependent claim 2. Accordingly, Appellants respectfully request withdrawal of the rejection of claims 1-2 under 35 U.S.C. § 102(b).

### 2. Examiner's Response and Appellants' Rebuttal

In the Office Action mailed July 23, 2008, the Examiner responds to the

above arguments by alleging:

> Applicant first argued that claim 1 differs from the Benantar reference in that the rules of claim 1 "specify if and how the data subject may be provided by the first data user to the second data user," in contrast to Benantar specifying what operations each user is allowed to perform on the data subject. The examiner respectfully disagrees, noting that figure 5 and column 6, lines 54-67 indicate that the user Alice is allowed to "administer" and "control" objects in group 2, and that users in the group programmers may "control" objects in group 2. Rules specifying administration of a data object implies the ability of the first user Alice to provide the data subject to a second user.
>
> With regards to claims 2, 3, and 19, the applicant similarly cited that the "rules" of claim 1 were not anticipated alone or in combination with either Tolopka or Gifford. The examiner respectfully disagrees, for the reason cited above.
> (July 23, 2008 Office Action, page 2)

Figure 5 of Benantar depicts the following:

FIG. 5

| | OBJGRP1 | OBJGRP2 |
|---|---|---|
| ALICE | READ, WRITE, EXECUTE | USE, ADMINISTER, CONTROL |
| PROGRAMMERS | EXECUTE | USE, CONTROL |
| GUEST | READ | USE |

Column 6, lines 54-67 reads as follows:

> The objects are grouped in accordance with access control policies such as is shown in greater detail in FIG. 5. For object group

> 1, an owner (Alice) is authorized to read, write and execute relative to any object in object group 1. Users identified as "programmers" are by policy limited to execute only. Users identified as "guests" are limited by policy to read only.
>
> The policies in object group 2 relate to use, administration, and control of access. Again, the owner (Alice) may use, administer, or control the objects in accordance with the policies set forth for object group 2. Programmers may use or control but may not administer in accordance with the policies set forth for object group 2. Guests may use but may not control nor administer.

All that these sections of the Benantar reference teach is that different levels of access to objects in object groups may be provided to different users. In the example, Alice has a different level of access than the "programmers" or the "guests." While this section mentions levels of access including read, write, execute, use, administration, and control, there is no teaching or suggestion in Benantar regarding what these various levels of access entail. Thus, the Examiner's allegation that simply because the word "administrate" appears as one level of access that this somehow necessarily teaches that the user "Alice" is able to "provide the data subject to the second user" is erroneous.

Benantar is not concerned with specifying what types of operations may be performed by a user having "administration" level of access to a group of objects. To the contrary, all that Benantar is trying to show by Figure 5 and the corresponding section in column 6, lines 54-67 is that different levels of access may be assigned to different users for the various object groups. Again, Benantar's contribution is to optimize the storage of access control lists by grouping objects for which the access levels are the same. Since Benantar does not teach what is involved in having "administration" level access and is not concerned with what operations may be performed by a user having

"administration" level access, the Examiner's allegation that this must necessarily allow the user to provide the data subject, i.e. the group of objects, to a second user is simply without merit. At the very least, due to this lack of teaching in Benantar, the Benantar reference does not identically teach each and every feature of independent claim 1 as is required under 35 U.S.C. § 102(b).

Moreover, the "rules" features of claim 1 are not obvious in view of Benantar for similar reasons. There is absolutely no teaching or even suggestion as to what it means to have "administration" level access to an object group in Benantar other than that this level of access is somehow different from the other levels of access mentioned in Benantar. The Benantar reference could just as easily have referred to access levels 1, 2, 3,...etc. and taught as much as what it currently does with regard to what is involved in "administration," "use," and "control" levels of access, i.e. these are only labels used to show a difference in levels of access, not specific types of operations that can be performed within these different levels of access.

The only way that one would read such "rules" features of claim 1 into the Benantar reference is to have a prior knowledge of Appellants' claimed invention and the sole intent of attempting to recreate Appellants' claimed invention from the Benantar reference, despite the actual teachings and lack of teachings in Benantar, based on such prior knowledge of Appellants' claimed invention. This is impermissible hindsight reconstruction using Appellants' own disclosure as a guide.

Thus, for the reasons set forth above, Appellants respectfully submit that the Benantar reference does not teach each and every feature of independent claim 1 as is required under 35 U.S.C. § 102(b) and the features emphasized above with regard to claim 1 are also not obvious under 35 U.S.C. § 103(a) based on the

Benantar reference. At least by virtue of its dependence on claim 1, Benantar does not teach or suggest the features of dependent claim 2 for similar reasons as noted above. Accordingly, Appellants respectfully request that the Board of Patent Appeals and Interferences overturn the rejection of claims 1-2 set forth in the Office Action.

### B. Rejection under 35 U.S.C. §103(a) of Claim 3

The Office Action rejects claim 3 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Benantar in view of Tolopka (U.S. Patent No. 6,044,349). This rejection is respectfully traversed for at least the same reasons as set forth above with regard to the 35 U.S.C. § 102(b) rejection based on Benantar. That is, as first submitted in the Response to Final Office Action filed April 1, 2008 and entered with the RCE filed April 25, 2008, Benantar does not teach or even suggest the features discussed above. Moreover, Tolopka does not provide any teaching or suggestion to alleviate the deficiencies of Benantar noted above.

Tolopka is directed to a portable storage medium to store data and provide access to information from an information dissemination system (IDS). The storage medium can store one or more location/key pairs. Each of the location/key pairs designates a particular IDS location as well as an access key to the particular IDS location. The storage medium can also store a plurality of information units. The information units are categorized into levels of information categories with at least one information category per level and at least one information unit per information category. Levels of information categories can be individually accessed and categories of information units within levels can be selectively downloaded.

Thus, Tolopka is only concerned with what access a particular information seeking system has to an IDS, and controls this access based on a key providing on a smart card. The key and smart card in Tolopka operate in a similar manner as the ACLs of Benantar in that they only control access by that particular subject, or information seeking system, to a particular object. They do not have anything to do with controlling how the information seeking system may then send that information to another information seeking system.

Tolopka is cited by the Office Action as allegedly teaching objects that may represent paper-filled forms (Office Action, page 5) at column 6, lines 36-52. As presented here for the first time, Appellants respectfully submit that this section of Tolopka states that the user may manually type information with a text editor or other application and download it to the storage medium such that user entered labels, and apparently the data, may be added to the table shown in Figure 2, which is a depiction of information categories and information units stored on the storage medium (see Tolopka, Brief Description of the Drawings). Simply because the user can add labels and data to a data structure, which is depicted as a table in Figure 2, does not mean that Tolopka teaches an object class having rules associated with data that represents a filled paper form including both collected data and rules regarding the collected data, as recited in claim 3. The table in Figure 2 of Tolopka is not an object class representing a filled paper form and furthermore, does not include both collected data and rules regarding the collected data.

However, as first presented in the Response to Final Office Action filed April 1, 2008 and entered with the RCE filed April 25, 2008, even if Tolopka were interpreted somehow to teach or suggest such features, Tolopka does not provide any teaching or suggestion regarding rules that define if and how the personally

identifiable information (about a data subject) may be provided, by a first data user, to a second data user, as recited in independent claim 1, from which claim 3 depends. Thus, any alleged combination of Tolopka and Benantar, even if such a combination were possible and one were somehow motivated to make such a combination of teachings, would not result in the features of independent claim 1, or its dependent claim 3, being taught or suggested. That is, the alleged combination still suffers from the deficiencies of Benantar discussed at length above with regard to the rejection under 35 U.S.C. § 102(b).

In response to these arguments, the Examiner merely responds by pointing to the Examiner's reasoning regarding the "rules" of the present claims as set forth with regard to claim 1 discussed above (see July 23, 2008 Office Action, page 2). Appellants have shown the error of the Examiner's position with regard to the features of claim 1 above. Furthermore, this does not address the deficiencies of Tolopka with regard to actually teaching or suggesting an object class representing a filled form having collected data and rules associated with the collected data, as discussed above.

In view of the above, Appellants respectfully submit that the alleged combination of Benantar and Tolopka does not teach or suggest the features of claim 3. Accordingly, Appellants respectfully request that the Board of Patent Appeals and Interferences overturn the rejection of claim 3 under 35 U.S.C. § 103(a) set forth in the Office Action.

### C. Rejection under 35 U.S.C. §103(a) of Claim 19

The Office Action rejects claim 19 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Benantar in view of Gifford (U.S. Patent No.

5,614,927). This rejection is respectfully traversed for at least the same reasons as set forth above with regard to the 35 U.S.C. § 102(b) rejection based on Benantar. That is, Benantar does not teach or even suggest the features discussed above with regard to independent claim 1, from which claim 19 depends. Moreover, Gifford does not provide any teaching or suggestion to alleviate the deficiencies of Benantar noted above.

As first presented in the Response to Final Office Action filed April 1, 2008 and entered with the RCE filed April 25, 2008, Gifford is directed to a system and method for protecting a database against deduction of confidential attribute values therein. A memory is provided for storing the database and a processor is provided for processing the database. Using the processor, the database is electronically partitioned into public attributes, containing non-confidential attribute values, and private attributes, containing private attribute values. The processor is then used to electronically process the private attribute values to reduce any high correlation between public attribute values and private attribute values.

Gifford is cited by the Office Action as allegedly teaching depersonalization of objects (see July 23, 2008 Office Action, pages 5-6) at column 8, lines 1-8. As presented here for the first time, column 8, lines 1-8 teaches that after partitioning a database, the correlation between public attributes and private attributes is reduced by camouflaging some highly correlative public attribute values and outright removing some tuples containing highly correlative public attribute values which are difficult to camouflage. Camouflaging the correlation between a public attribute and a private attribute in a partitioned database does not teach or suggest transforming, based on rules, personally identifiable information into a **depersonalized format prior to providing the personally identifiable**

**information to the second data user**. All that Gifford teaches is that the link between one attribute and another is camouflaged.

However, as discussed in the Response filed April 1, 2008, even if Gifford were somehow interpreted to teach or suggest such features in claim 19, Gifford still does not provide any teaching or suggestion regarding rules for governing if and how a first data user may send a data subject to a second data user. Thus, any alleged combination of Gifford and Benantar, even if such a combination were possible and one were somehow motivated to make such a combination of teachings, would not result in the features of independent claim 1, or its dependent claim 19, being taught or suggested.

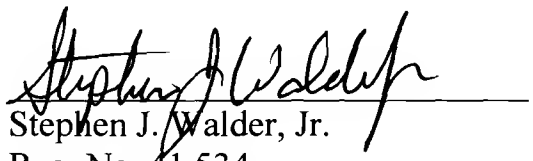
Again, in response to these arguments the Examiner merely responds by pointing to the Examiner's reasoning regarding the "rules" of the present claims as set forth with regard to claim 1 discussed above (see July 23, 2008 Office Action, page 2). Appellants have shown the error of the Examiner's position with regard to the features of claim 1 above. Furthermore, this does not address the deficiencies of Gifford with regard to actually teaching or suggesting transforming, based on rules, personally identifiable information into a **depersonalized format prior to providing the personally identifiable information to the second data user**, as discussed above.

In view of the above, Appellants respectfully submit that the alleged combination of Benantar and Gifford does not teach or suggest the features of claim 19. Accordingly, Appellants respectfully request that the Board of Patent Appeals and Interferences overturn the rejection of claim 19 under 35 U.S.C. § 103(a) set forth in the Office Action.

## D. Conclusion

In view of the above, Appellants respectfully submit that claims 1-3 and 19 of the present application are not taught or suggested by the Benantar, Tolopka, or Gifford references, whether taken alone or in combination. Accordingly, Appellants request that the Board of Patent Appeals and Interferences overturn the rejections set forth in the July 23, 2008 Office Action.

Respectfully submitted,



Stephen J. Walder, Jr.
Reg. No. 41,534
**Walder Intellectual Property Law, P.C.**
17330 Preston Road, Suite 100B
Dallas, TX 75252
Phone: (972) 380-9475
Fax: (972) 733-1575
Email: swalder@walderiplaw.com
ATTORNEY FOR APPELLANTS

## X. Appendix

### A. Claims

1. (Rejected) A method, in a data processing system, for handling personally identifiable information, said method comprising:

providing, in a computer, a first set of object classes representing active entities in an information-handling process, wherein a limited number of privacy-related actions represent operations performed on data and wherein each of the active entities is a human being or legal entity;

providing, in said computer, a second set of object classes representing data and rules in said information-handling process, wherein at least one object class has said rules associated with said data, and wherein said data represents said personally identifiable information; and

processing transactions, in the data processing system, involving said personally identifiable information, using said computer and said first and second set of object classes, so as to enforce a privacy policy, associated with the personally identifiable information and defined by said rules, against one or more active entities represented by said first set of object classes, wherein each of the one or more active entities represented by said first set of object classes is a human

being or legal entity, wherein:

a first active entity represented by a first object class in said first set of object classes is a first data user that requests said personally identifiable information from a data subject that is a second active entity represented by a second object class in said first set of object classes,

said data subject is an active entity that is personally identifiable by said personally identifiable information;

a third active entity represented by a third object class in said first set of object classes is a second data user that requests said personally identifiable information from said first data user, and

said rules define if and how said personally identifiable information may be provided, by said first data user, to said second data user.

2. (Rejected) The method of claim 1, wherein said first set of object classes include one or more object classes representing parties, selected from the group consisting of

a data user object class,

a data subject object class,

a guardian object class, and

a privacy authority object class.

3. (Rejected) The method of claim 1, wherein said at least one object class, having said rules associated with said data, represents a filled paper form, including both collected data and rules regarding said collected data.

4-18. (Canceled)

19. (Rejected) The method of claim 1, further comprising:

transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user.

20-22. (Canceled)

## B. Claims Support and Drawing Analysis

1. (Rejected) A method **{e.g., Figure 2; page 10, lines 3-5; Figure 3; page 10, lines 17-20; Figure 4; page 11, lines 23-26; Figure 5; page 12, lines 17-20}**, in a data processing system **{e.g., page 6, line 28 to page 7, line 1; Figure 1}**, for handling personally identifiable information **{e.g., page 8, lines 23-29; 503 in Figure 5; page 12, lines 24-26; 910 in Figure 9; page 28, lines 15-17}**, said

method comprising:

providing, in a computer **{e.g., Figure 1}**, a first set of object classes **{e.g., 601, 602, 605 in Figure 6; 701, 703, 702 in Figure 7}** representing active entities in an information-handling process **{e.g., data subject 301, data user 303, data user 305 in Figure 3; page 10, line 28 to page 11, line 1}**, wherein a limited number of privacy-related actions represent operations performed on data **{e.g., page 11, lines 14-18}** and wherein each of the active entities is a human being or legal entity **{e.g., page 10, line 28 to page 11, line 1}**;

providing, in said computer, a second set of object classes **{e.g., 706 and 707 in Figure 7}** representing data and rules **{e.g., 204 in Figure 2; page 10, lines 8-12; 404 in Figure 4; page 12, lines 3-5}** in said information-handling process **{e.g., 304 in Figure 3; page 10, lines 20-23}**, wherein at least one object class has said rules associated with said data **{e.g., page 11, lines 4-6 and 13-14}**, and wherein said data represents said personally identifiable information **{e.g., 705 in Figure 7}**; and

processing transactions, in the data processing system, involving said personally identifiable information **{e.g., see example transactions shown in Figure 10}**, using said computer and said first and second set of object classes, so as to enforce a privacy policy **{e.g., page 11, lines 2-4}**, associated with the personally identifiable information and defined by said rules **{e.g., page 11, lines 6**

**and 13-14}**, against one or more active entities represented by said first set of object classes **{e.g., page 11, lines 6-12}**, wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity **{e.g., page 10, line 28 to page 11, line 1}**, wherein:

a first active entity represented by a first object class in said first set of object classes is a first data user **{e.g., 1080 in Figure 10; page 30, line 25 to page 31, line 1}**; that requests said personally identifiable information from a data subject **{e.g., 801 in Figure 8; page 27, lines 6-8; page 30, line 25 to page 31, line 1}** that is a second active entity represented by a second object class **{e.g., 1060 in Figure 10}** in said first set of object classes,

said data subject **{e.g., 1060 in Figure 10; page 30, lines 16-20}** is an active entity that is personally identifiable by said personally identifiable information;

a third active entity represented by a third object class in said first set of object classes is a second data user **{e.g., 1090 in Figure 10}** that requests said personally identifiable information from said first data user **{e.g., page 30, line 25 to page 31, line 1}**, and said rules define if and how said personally identifiable information may be provided, by said first data user, to said second data user **{e.g., page 12, lines 6-15; page 22, lines 16-21; page 31, lines 2-9}**.

2. (Rejected) The method of claim 1, wherein said first set of object classes include one or more object classes representing parties, selected from the group consisting of

a data user object class **{e.g., 303 or 305 in Figure 3; 605 in Figure 6}**,

a data subject object class **{e.g., 301 in Figure 3; 602 in Figure 6}**,

a guardian object class **{e.g., 603 in Figure 6}**, and

a privacy authority object class **{e.g., 604 in Figure 6}**.

3. (Rejected) The method of claim 1, wherein said at least one object class, having said rules associated with said data, represents a filled paper form **{e.g., 304 in Figure 3; page 10, lines 20-23; page 11, lines 4-6; 707 in Figure 7; 1070 in Figure 10; page 31, lines 4-5}**, including both collected data and rules regarding said collected data **{e.g., page 10, lines 26-28; page 11, lines 4-6}**.

19. (Rejected) The method of claim 1, further comprising:

transforming, based on said rules, said personally identifiable information into a depersonalized format **{e.g., 505 in Figure 5; page 13, lines 6-12; page 33, lines 3-5}** prior to providing said personally identifiable information to the second data user **{e.g., page 14, lines 4-7}**.

## C. Means or Step Plus Function Analysis

NONE

## D. Evidence

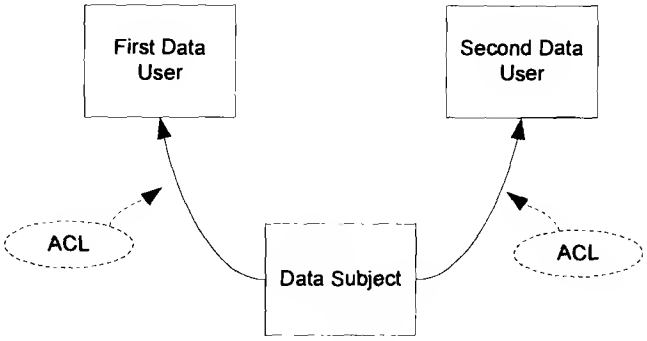



FIGURE A

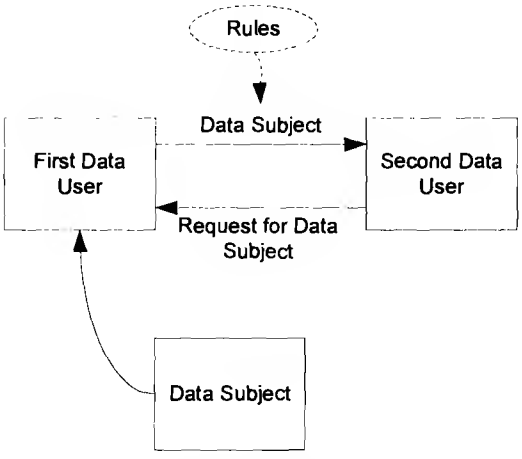



FIGURE B

## E. Related Cases

NONE